NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Fire threatens Minn-Dak Farmers Co-op. Minn-Dak Farmers Co-op security reported a fire May 29. The inferno started on a conveyor belt system, said the Richland County, North Dakota emergency manager. When firefighters arrived, they found the fire had spread to an adjacent wall and was nearing a 40-foot sulfur tank, he said. Fire crews from Dwight and Wahpeton stopped the fire from reaching the tank and spreading poisonous gasses into the air. About an hour into their fight, crews had contained the fire. About 75-80 firefighters were on the scene. Richland County highways 30 and 87 were temporarily closed due to the fire and for public safety, the emergency manager said. Source: http://www.wahpetondailynews.com/news/article_ff6819c4-aa63-11e1-9a97-0019bb2963f4.html

Former Dickinson bank officer to plead guilty to fraud today. A former trust officer at a Dickinson, North Dakota bank was scheduled to plead guilty to conspiracy to commit bank fraud May 30. The trust officer is accused of plotting with her husband to steal almost $750,000 from five clients at the Bank of the West. Federal court documents said most of the money was funneled to the officer's sister and nephew. Court records said she also conspired to take over one client's mineral interests in four western North Dakota counties. The officer is accused of stealing more than $130,000 from her. She has reached a plea agreement with prosecutors and is scheduled to plead guilty in federal court in Bismarck. Her husband has already pleaded guilty. Source: http://www.thedickinsonpress.com/event/article/id/58503/group/homepage/

Regional

(Minnesota) **State apple crop takes hit.** The 2012 apple crop suffered "major damage" according to an update from the Minnesota Department of Agriculture, the Minneapolis Star Tribune reported May 25. The damage occurred after a balmy March jump-started the bloom cycle, then freezing temperatures in April nipped the delicate blossoms at a critical stage. Growers waited during April and May for pollination to reveal more about the fate of the apple crop. Many had guessed, based on early blossom damage, that losses would be severe. Now that fruit has formed, damage reports vary widely, with some growers reporting only minimal losses and others, anticipating they would be able to produce only a small fraction of yields compared to 2011. Source: http://www.startribune.com/local/154302905.html

(Montana) **Pipeline Safety Review Council releases report.** A Montana panel released its report with recommendations for changes in the wake of the 2011 oil spill into the Yellowstone River, KTVH 12 Helena reported May 29. Among their suggestions were technology upgrades by companies and more money for pipeline inspectors. The council chairman said none of the recommendations were binding, with most falling outside State jurisdiction. Montana's governor formed the council after a 1,500 barrel crude oil spill from an Exxon Mobil pipeline near Laurel. Source: http://www.beartoothnbc.com/news/montana/22849-pipeline-safety-review-council-releases-report.html

(South Dakota) **Stripe rust found in South Dakota.** Stripe rust was found on winter wheat in several South Dakota locations the week of May 21, South Dakota State University (SDSU) reported May 31. The U.S. Department of Agriculture Cereal Disease Lab reported stripe rust appeared at nearly the same time in Minnesota, North Dakota, Wisconsin, and Ontario, Canada, suggesting there were likely one or more recent very large spore shower events. If cool, wet conditions persist, stripe rust can be expected to spread aggressively, whereas warm temperatures and dry conditions will cause it to shut down, said a SDSU Extension plant pathology field specialist. Source: http://www.agprofessional.com/news/Stripe-rust-found-in-South-Dakota-155773445.html?ref=445

(South Dakota) **Health department trains for disease outbreaks.** The South Dakota Health Department will work with hospitals, clinics, and other facilities in a Statewide training exercise May 31 for dealing with disease outbreaks and other emergencies. The training exercise will involve a mock outbreak of Hantavirus, a viral infection spread by mice and rats. A spokesman for the health department said the training exercise is a practice run for responding to an actual emergency. He said it gives officials a chance to test response plans that include communication, hospital evacuation, and the management of resources and volunteers. The federal DHS and many local, regional, and State emergency managers will take part in the training exercise.Source: http://www.ksfy.com/story/18635134/health-department-trains-for-disease-outbreaks

National

Some early-planted corn showing signs of seedling blights. Many eastern corn belt fields in the U.S. midwest planted in mid-April when farmers got off to an early start have started to show symptoms of seedling blights, said a Purdue Extension plant pathologist, USAgNet reported May 29. Symptoms include uneven stands, stunted seedlings, or reduced plant vigor. They can be caused by a number of scenarios, such as damage from cold temperatures, nutrient deficiencies, herbicide or anhydrous ammonia injury, wireworms or “wet feet,” but also could be caused by seedling blights from fungi or fungal-like organisms. “Seedling blights are prevalent when cool, wet soil conditions persist after planting,” said an official. Most farmers planted into dry soils in 2012, but the mid- to late-April cool-down lowered soil temperature and slowed corn emergence. Rain in late April and early May likely increased stress and allowed fungal organisms to infect and damage seedlings, the official said. Many different types of soil or seed fungi can cause blights. They can cause seeds to rot after germination, either preventing emergence or stunting root development in plants that do emerge. Source: http://www.wisconsinagconnection.com/story-national.php?Id=1209&yr=2012

International

Nothing Significant to Report

Banking and Finance Industry

Romanian extradited in computer scheme that allegedly stole credit card info at U.S. cash registers. A Romanian man was extradited to the United States to face charges that he was part of a fraud ring that allegedly electronically accessed as many as 80,000 credit cards while they were being used at cash registers across the country, Government Security News reported May 30. The charges allege the man participated in a scheme to remotely steal payment card data from hundreds of U.S. merchants' "point of sale" (POS) computer systems. An indictment handed down in December 2011 charged the man and three other Romanian nationals ran the computer fraud conspiracy. Federal authorities allege that between 2008 and May 2011, the men conspired to remotely hack into more than 200 U.S.-based POS systems at stores across the U.S. to steal credit, debit, and gift card numbers and associated data. Merchant victims included more than 150 Subway restaurant franchises, the U.S. Department of Justice said. According to the indictment, millions of dollars of unauthorized purchases have been made using the compromised data. Source: http://www.gsnmagazine.com/node/26455?c=cyber_security

123,000 Thrift Savings Plan accounts hacked. Social Security numbers and other personal data for 123,000 Thrift Savings Plan (TSP) account holders were stolen from a contractor's computer in 2011, a TSP spokeswoman said May 25. Names, addresses, and financial account and routing numbers of some accounts were also compromised. A spokeswoman for the Federal Retirement Thrift Investment Board, which manages the TSP program, said the hacking incident targeted a computer operated by contractor Serco Inc., which provides record-keeping services for 4.5 million federal employees, service members, and beneficiaries with TSP accounts. "It was a sophisticated attack that overcame the defenses [Serco] had in place," the spokeswoman said. She aid both TSP and Serco have enhanced their cybersecurity. "We have monitored our TSP accounts, [and] we have no reason to believe that the data was misused in any way." The attack occurred in July 2011, but the Federal Retirement Thrift Investment Board and Serco were not aware of it until they were notified in April 2012 by the FBI, the spokeswoman said. The infected computer was immediately shut down and the security of all TSP and Serco systems was reviewed. Source: http://www.militarytimes.com/news/2012/05/federal-tsp-accounts-hacked-last-year-052512/

SIGTARP, CFPB, and Treasury issue a fraud alert to the Armed Services community to combat HAMP mortgage modification scams. The Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), the Consumer Financial Protection Bureau (CFPB), and the U.S. Department of the Treasury (Treasury) May 24 issued a fraud alert to the Armed Services community to combat scams targeted at homeowners seeking to apply for mortgage assistance through the Home Affordable Modification Program (HAMP) and other federal programs. Many of these scams are specifically targeting members of the Armed Services community. The fraud alert is designed to raise awareness of the scams and provides a list of resources available for more information and for assistance with mortgage-related questions and how to report fraud. Hallmarks of HAMP mortgage-modification scams include: the unofficial use of official program names or logos of government agencies, non-profit

organizations, and/or lenders; the advertising of a very high success rate in achieving modifications; and the guarantee of a successful modification in exchange for an upfront fee. Source: http://www.treasury.gov/press-center/press-releases/Pages/tg1592.aspx

Chemical and Hazardous Materials Sector

GAO suggests risk assessment for nuclear plants needs improving. The Government Accountability Office (GAO) concluded the methods used to determine natural hazard risks at the nation's nuclear power plants could be improved, the San Luis Obispo Tribune reported May 31. In a highly technical report issued the week of May 28, the GAO said the Nuclear Regulatory Commission should review the benefits of requiring that nuclear plants add probabilistic risk assessment to the methods used to evaluate and prepare for natural hazards such as earthquakes and tsunamis. Probabilistic risk assessment is a broader method for assessing what can go wrong, its likelihood, and its potential consequences. Findings would help determine levels of risk to provide insights into the strengths and weaknesses of the design and operation of a nuclear power reactor. Source: http://www.sanluisobispo.com/2012/05/30/2086602/gao-suggests-risk-assessment-for.html

Commercial Facilities

(Indiana) **2 dead in Indianapolis shooting spree.** A gunman opened fire at an Indianapolis apartment complex May 30, fatally shooting a woman and critically wounding three other people before turning the gun on himself as officers confronted him, police said. An employee in the leasing office was shot and killed. Two other women and a maintenance man also were shot. All were in critical condition at local hospitals. Police had no information about a possible motive but believed the gunman lived at the complex. Source: http://www.courier-journal.com/viewart/20120530/NEWS02/305300104/2-dead-Indianapolis-shooting-spree

(Washington) **Shootings stun Seattle residents; gunman, 5 victims dead.** A man in Seattle killed five people in two shootings before turning the gun on himself, CNN reported May 31. The suspect died several hours after he shot himself in the head as a 5-hour police manhunt came to an end May 30. Detectives believed the man was behind both shootings. The first, at a coffeehouse in the city's University District, left four people dead and one critically injured. The second occurred about 30 minutes later near downtown Seattle, when a woman was shot dead in what police described as a possible carjacking. Source: http://www.cnn.com/2012/05/31/us/washington-cafe-shooting/index.html?hpt=hp_t2

(Colorado) **9 evacuated from southwest Colorado gondola cars.** Officials in Mountain Village, Colorado, said nine people and a dog had to be lowered from gondola cars when a gearbox problem caused the system to shut down May 29. The Telluride Daily Planet reported that rescuers used ropes and harnesses to get the passengers out of eight cars and down to the ground. Crews waited an hour to begin the evacuation in case the gondola could restart. It took another 1 hour and 45 minutes to get everyone out. The 3-mile-long gondola connects Telluride and Mountain Village, carrying skiers, hikers, and sightseers. Source:

http://www.stltoday.com/news/national/evacuated-from-southwest-colorado-gondola-cars/article_1d79ed6a-066b-5307-bef1-1831445b03c0.html

Communications Sector

Nothing Significant to Report

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

(Maine) **Navy: 2-3 weeks for answers on fired-damaged sub.** May 29, a union leader said he is confident the fire-damaged USS Miami can be repaired, but it will be several weeks before the U.S. Navy reaches conclusions on the extent of damage. The Navy will provide an update on the nuclear-powered submarine after three separate investigations are completed in 2 to 3 weeks, a spokeswoman for the Naval Sea Systems Command said May 29. Based in Connecticut, the Los Angeles-class submarine was in dry dock at Portsmouth Naval Shipyard in Kittery, Maine, for an overhaul when a fire broke out the week of May 21, damaging forward compartments including the torpedo room, command and control, and crew quarters, officials said. An investigation by the military's legal arm, the Judge Advocate General Corps, will investigate what caused the fire, while a separate team is looking at safety procedures. The Naval Criminal Investigative Service is looking into whether a crime was committed. Source: http://www.boston.com/news/local/new_hampshire/articles/2012/05/29/navy_2_3_weeks_for_answers_on_fired_damaged_sub/

UK researchers discover backdoor in American military chip. United Kingdom (U.K.)-based security researchers found a backdoor "deliberately" inserted into an American military chip to help attackers gain unauthorized access and reprogram its memory, according to a draft research paper. A researcher at Cambridge University discovered a military-grade silicon device made by California-based Microsemi Corp., the ProASIC3 A3P250, contained a glitch that would allow individuals to remotely tweak its functions. He collaborated with a researcher at U.K.-based Quo Vadis Labs, which researches sensor technology, and found "proof that the backdoor was deliberately inserted and even used as a part of the overall security scheme." The duo did not disclose details, citing a "confidentiality agreement." The backdoor is "close to impossible to fix on chips already deployed" because software patches cannot fix the bugs. The holes can only be removed by removing all such chips installed in systems, the duo said. Microsemi's aggregate net sales to defense and security users represented about 29 percent of total net sales in 2012, according to its most recent quarterly regulatory filing. The device in question is "heavily marketed to the military and industry," the draft report states. Source: http://www.nextgov.com/defense/2012/05/uk-researchers-discover-backdoor-american-military-chip/55949/

Emergency Services

(California) **Fremont woman found dead in car in apparent suicide using hazardous chemicals.** A woman died in an apparent suicide in Freemont, California, May 30 in a car that contained a poisonous substance in an apartment parking garage, causing the garage to be shut down and a shelter-in-place order to be issued. She was sitting in the back seat next to a container of hydrogen sulfide, a flammable colorless gas that can be made from mixing household cleaning liquids. A sign on the vehicle's windshield said, "poison gas," and a strong odor similar to that of rotten eggs was present. A shelter-in-place order was issued for the apartment complex's residents, and Civic Center Drive was closed to traffic between Walnut Avenue and Stevenson Boulevard. The poisonous compound was removed and authorities reopened street traffic and lifted the shelter-in-place order after about 4 hours. Authorities closed the apartment complex parking garage for most of the day while detectives and the hazardous materials crew investigated. Source: http://www.insidebayarea.com/news/ci_20741070/fremont-crews-respond-hazmat-scene-at-parking-garage?source=most_emailed

Energy

Nothing Significant to Report

Food and Agriculture

(New Mexico) **USDA gives green light to Mexican cattle.** Livestock are expected to once again cross into the United States from Mexico at New Mexico's Columbus Port of Entry starting the week of June 4, the New Mexico Department of Agriculture said May 30. The port, which processes 70,000 Mexican cattle a year, has been closed to Mexican cattle since March when the Agriculture Department restricted its veterinarians from traveling to Mexico to inspect the cattle. At the time, the U.S. Department of Agriculture said it was concerned the veterinarians were working in unsafe facilities on the Mexican side of the border. Mexican livestock must be inspected by U.S. veterinarians on the Mexican side of the port to ensure they are disease-free. U.S. cattle feeding lots frequently purchase "feeder" cattle from Mexico to supplement their herds. U.S. ranchers often sell breeding stock to Mexican ranchers. Source: http://www.bizjournals.com/albuquerque/news/2012/05/30/usda-gives-green-light-to-mexican-cattle.html

After eight expansions, how big is the Diamond Pet Foods recall? A U.S. Food and Drug Administration (FDA) spokeswoman said the Salmonella contamination found at the Meta, Missouri plant of Diamond Pet Foods was not from the same strain as that of the Gaston, South Carolina plant, Food Safety News reported May 29. The contamination at the Missouri plant comes from Salmonella Liverpool, while the South Carolina plant — connected to all products except those in the most recent recall expansion — was contaminated by Salmonella Infantis. The spokeswoman also said the Missouri plant has now been included in the FDA's ongoing investigation into the Diamond Pet Foods Salmonella outbreak and recall. Source:

http://www.foodsafetynews.com/2012/05/after-eight-expansions-how-big-is-the-diamond-pet-foods-recall/

Chicken of the Sea recalls Korean oysters. Chicken of the Sea International of San Diego recalled several product codes of oysters imported from Korea and sold under the Chicken of the Sea, Pacific Pearl, and Ace of Diamonds brands, Food Safety News reported May 29. The recall was based on findings by the Food and Drug Administration of unsanitary conditions in the processing of shellfish at specified plants in Korea. The recall is for: Chicken of the Sea Whole Oysters; Chicken of the Sea Oyster Pieces; PacificPearl Whole Oysters; Ace of Diamonds Whole Oysters; and Pacific Pearl Smoked Oyster Water. Source: http://www.foodsafetynews.com/2012/05/chicken-of-the-sea-recalls-korean-oysters/

Thirsty crops need more than a shower. From plains wheat country to the eastern corn belt, there was a lot riding on rainfall chances the weekend of May 26. The last several weeks saw just fractions of normal rainfall in the Nation's midsection, leading to both growing shortages of soil moisture and declining crop conditions. The U.S. Drought Monitor showed how rapidly the dry conditions were spreading. As of May 22, virtually all of Iowa, Minnesota, and Kansas ranges from abnormally dry to moderate drought, with about half of Missouri and Illinois under similar conditions. "Drought conditions expanded considerably across the Midwest, northern Delta and central Plains, with dry conditions now being noted in north-central Kansas, eastern Oklahoma, much of Arkansas, southern Missouri, southern Illinois, western Kentucky, Iowa, Minnesota, and eastern North Dakota," said the MDA EarthSat Weather senior ag meteorologist. Source: http://www.agriculture.com/news/crops/thirsty-crops-need-me-th-a-shower_2-ar24326

Government Sector (including Schools and Universities)

(Virginia) **Alleged white supremacist from Manassas arrested for illegally possessing fully automatic AK-47.** An alleged white supremacist from Manassas, Virginia, who has expressed hatred and support for violence toward many political figures was arrested May 30 by FBI Joint Terrorism Task Force agents and accused of illegally obtaining a fully automatic AK-47. The 48-year-old man was charged with making a firearm in violation of the National Firearms Act. A confidential source saw information the suspect posted on an Aryan Nation Web site indicating he was preparing to buy an AK-47 and have it modified to become fully automatic. He allegedly stated he was planning on ambushing and murdering any law enforcement officer that stopped him on the street if and when martial law is enacted. In addition, he allegedly made numerous statements on various white supremacy online forums, including his desire that the U.S. President and Attorney General be removed from office "with a 30.06." Source: http://www.fbi.gov/washingtondc/press-releases/2012/alleged-white-supremacist-from-manassas-arrested-for-illegally-possessing-fully-automatic-ak-47

NASA denies Iranian cyberattack. NASA denied May 25 that its Web site had been hacked and information stolen by a band of Iranian students that called themselves the "Cyber Warriors Team." The group bragged in a May 16 post on Pastebin that it had hacked a NASA site and stolen the personal information of thousands of NASA researchers. The site allegedly compromised is called the Solicitation and Proposal Integrated Review and Evaluation System. NASA said it discovered the Pastebin post within hours and launched an investigation of the claims. "Although the investigation is ongoing, all results thus far indicate that the claims are false," a NASA spokeswoman said. On the same day as the alleged Iranian hack, two other groups claimed on Pastebin to have broken into NASA systems. "They were also found to be false," she said. Source: http://www.csoonline.com/article/707073/nasa-denies-iranian-cyberattack

Information Technology and Telecommunications

DHS to critical infrastructure owners: Hold on to data after cyber attack. The DHS is offering organizations that use industrial control systems advice on mitigating the effects of cyber attacks. Among the agency's recommendations: Hold on to data from infected systems and prevent enemies from moving within your organization. DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published a technical paper on cyber intrusion mitigation strategies May 25. The document calls on critical infrastructure owners to take a number of steps to thwart attacks, or limit the damage they cause. Among them are improving their ability to collect and retain forensic data, and to detect attempts by attackers to move laterally within their organization. The document is guidance from ICS-CERT to critical infrastructure owners and is targeted at both enterprise and control system networks, DHS said. Source: http://threatpost.com/en_us/blogs/dhs-critical-infrastructure-owners-hold-data-after-cyber-attack-052912

Administration unveils plan for battling botnets. The U.S. Government and a private-sector working group announced a cooperative initiative to combat malicious botnets, which are being called a growing threat to the online economy and national security. May 30, the Industry Botnet Group and DHS and the Commerce Department released a set of principles for addressing the challenge of botnets across the Internet ecosystem. In addition to this framework for collaboration, the Government also will step up public outreach efforts to educate users about online threats and will coordinate efforts to address the technical threats posed by botnets. May 30, the National Institute of Standards and Technology hosted a workshop on the technical aspects of botnet activity, aimed at disrupting the botnet life cycle and removing malicious code on compromised devices. Source: http://gcn.com/articles/2012/05/30/anti-botnet-initiative-dhs-commerce.aspx

Nearly a fifth of U.S. PCs have no virus protection, McAfee finds. A McAfee study of PCs around the world found that 17 percent had no antivirus protection, and the United States outpaced the average with 19 percent of PCs unprotected. The study counted as unprotected machines those that had no antivirus protection installed, or whose antivirus subscription expired. In the United States, 12 percent of PCs did not contain an antivirus program, and 7

percent had expired software. McAfee analyzed data from voluntary scans of 27 million machines in 24 countries. According to the company, the study was the first to examine machines directly rather than polling their users. User polls typically found that 6 percent of PCs are not protected by antivirus software, McAfee's director of global consumer product marketing said. Source: http://www.pcworld.com/businesscenter/article/256493/nearly_a_fifth_of_us_pcs_have_no_virus_protection_mcafee_finds.html

No more dot-mil accounts on dating sites. According to Defense Department officials, the Pentagon plans to distribute a new policy on personal social media use that tells troops to hide certain identifying information when interacting online, Nextgov reported May 25. The directive was expected to be released in late May. Increasingly, hackers are gleaning sensitive work details from social networks by drawing inferences from posts, such as military unit locations, and by penetrating the actual sites. Defense officials acknowledged they are aware of a reported MilitarySingles.com breach that may have exposed soldiers' dot-mil e-mail addresses and passwords. Future instruction that specifically addresses use of commercial social media will direct all Defense employees to "use non-mission related contact information, such as telephone numbers or postal and email addresses, to establish personal accounts, when such information is required." Despite the forthcoming policy, dot-mil e-mail addresses may still appear in some personal communications, partly because family members and guests using the Army Knowledge Online service are issued military addresses, a Defense spokesperson said.Source: http://www.nextgov.com/cybersecurity/cybersecurity-report/2012/05/no-more-dot-mil-accounts-dating-sites/55930/?oref=ng-voicestop

Researchers identify Stuxnet-like malware called 'Flame'. A new, highly sophisticated malware threat predominantly used in cyberespionage attacks against targets in the Middle East was identified and analyzed by researchers from several security companies and organizations. According to the Iranian Computer Emergency Response Team, the new piece of malware might be responsible for recent data loss incidents in Iran. Flame, as the Kaspersky researchers call it, is a very large attack toolkit with many individual modules. It can perform a variety of malicious actions, most of which are related to data theft and cyberespionage. Among other things, it can use a computer's microphone to record conversations, take screenshots of particular applications when in use, record keystrokes, sniff network traffic, and communicate with nearby Bluetooth devices. One of the toolkit's first versions was likely created in 2010 and its functionality was later extended by leveraging its modular architecture, said a chief malware expert at Kaspersky Lab. Flame spreads to other computers by copying itself to portable USB devices and also by exploiting a now-patched Microsoft Windows printer vulnerability that was also leveraged by Stuxnet. Source: http://www.computerworld.com/s/article/9227524/Researchers_identify_Stuxnet_like_malware_called_Flame

Malware intelligence system allow organizations to share threat information. As malware threats expand into new domains and increasingly focus on industrial espionage, Georgia Tech researchers are launching a new tool to help battle the threats: a malware intelligence system

that will help corporate and government security officials share information about the attacks they are fighting. A Georgia Tech news release reports the system, known as Titan, will be at the center of a security community which will help create safety in numbers as companies large and small add their threat data to a knowledge base that will be shared with all participants. Operated by security specialists at the Georgia Tech Research Institute, the system builds on a threat analysis foundation — including a malware repository that analyzes and classifies an average of 100,000 pieces of malicious code each day. Source: http://www.homelandsecuritynewswire.com/dr20120529-malware-intelligence-system-allow-organizations-to-share-threat-information

Comcast users phished by Constant Guard spam lure. Naked Security discovered a new phishing scam targeting customers of Comcast XFINITY cable Internet service. They became aware of the scam after the scammers used a reader's Gmail address to send the scam to their intended victims. A link in the e-mail points at a TinyURL which redirected victims to a compromised higher education institution Web site in India. Like many other sites that are compromised to host phishing pages, this one appears to have been compromised through vulnerable FrontPage server extensions. The fake page is an identical copy of the real Comcast XFINITY log-in page and includes a fully functional TRUSTe logo which may lend further credibility to the site. Source: http://nakedsecurity.sophos.com/2012/05/24/comcast-users-phished-by-constant-guard-spam-lure/

National Monuments and Icons

(New Mexico) **Forest wildfire becomes largest in NM history.** A massive wildfire that burned more than 265 square miles in the Gila National Forest became the largest fire in New Mexico history, fire officials confirmed May 30. The erratic fire grew overnight May 29 to more than 170,000 acres, surpassing a fire in 2011 that burned 156,593 acres in Los Conchas and threatened the Los Alamos National Laboratory, the nation's premier nuclear facility. The Gila forest fire was also the largest currently burning in the country. It formed the week of May 21 when two lightning-sparked fires merged in an isolated mountainous area in southwestern New Mexico, where it has destroyed about a dozen homes and prompted evacuations of nearby towns and health alerts for some of the State's largest cities. A fire information officer said that about 1,200 firefighters from around the State were battling the growing fire, but they continue to face low humidity and shifting winds. Source: http://www.sacbee.com/2012/05/30/4525545/forest-wildfire-becomes-largest.html

Postal and Shipping

(California) **Postal worker robbed of mail in Stockton.** Stockton, California police said three men duct-taped a U.S. mail carrier at gunpoint and robbed him of about 3,500 pieces of mail May 24. Police said the carrier was adjusting his cargo when the unidentified men approached. One pushed his head down and held a gun to him while another taped his hands behind his back. The third man served as a lookout. The men then made off with the mail, leaving the

carrier in his truck. Source: http://www.ktvn.com/story/18625741/postal-worker-robbed-of-mail-in-stockton

PUBLIC HEALTH

FDA warns of fake Teva ADHD drug as shortage continues. The U.S. Food and Drug Administration (FDA) warned patients about counterfeit versions of a Teva ADHD drug that is on the drug shortage list, in-Pharma Technologist reported May 30. Lab tests run by the FDA showed the Adderall (amphetamine and dextroamphetamine) bought online is devoid of the four official active pharmaceutical ingredients. Instead, the tablets contain tramadol and acetaminophen, APIs used in the treatment of acute pain. API supply problems at Teva have put Adderall on the shortages list, and the FDA said counterfeit drug producers may especially target treatments consumers are struggling to find legitimately. The FDA updated its shortages list to say Teva is still releasing Adderall when available. Source: http://www.in-pharmatechnologist.com/Ingredients/FDA-warns-of-fake-Teva-ADHD-drug-as-shortage-continues

Biosafety concerns for labs in the developing world. An inspection of dozens of biocontainment labs across the Asia-Pacific region found that nearly one-third of the biosafety hoods intended to protect workers from deadly pathogens did not work properly, according to biorisk experts, Nature reported May 22. The experts spoke at a meeting at London, England's Chatham House. Stringent biosafety and biosecurity rules are unworkable in many developing countries, where researchers often need to handle infectious agents such as anthrax and plague to protect public health but lack the infrastructure of the West, said a fellow at Chatham House's Global Health Security center. The weaknesses could have repercussions around the globe if pathogens were released. "The strength of a chain is based on its weakest link, and developing countries are the weakest link," said the former president of the Asia-Pacific Biosafety Association based in Singapore, which co-sponsored the inspection. Source: http://www.nature.com/news/biosafety-concerns-for-labs-in-the-developing-world-1.10687

Wisconsin reports pertussis surge as U.S. outbreaks continue. Pertussis outbreaks in several U.S. States continued to keep health officials busy offering vaccination advice, according to a news release issued May 23 by the Center for Infectious Disease Research and Policy. A moderator for ProMED mail, the online reporting system of the International Society for Infectious Diseases, commented the current rash of outbreaks probably has multiple causes, including vaccine exemptions, "general under-vaccination," and waning vaccine-induced immunity. The moderator cited studies by Dutch and Australian researchers that revealed antigenic changes in circulating strains of Bordetella pertussis, which may be contributing to a worldwide increase in cases. A New Mexico Department of Health epidemiologist told the Associated Press the vaccine is "the best protection we have against pertussis, but it's probably somewhere in the neighborhood of 80 to 85 percent effective." Source: http://www.cidrap.umn.edu/cidrap/content/other/news/may2312pertussis.html

20 million affected by health breaches. The U.S. Department of Health and Human Services' (HHS) tally of individuals affected by major healthcare information breaches since September 2009 now exceeds 20 million, according to GovInfoSecurity' analysis of the list, which now includes 435 incidents as of May 23. Recently reported incidents at Emory Healthcare and South Carolina Department of Health and Human Services, estimated to have affected a combined total of more than 675,000, have yet to make the list pending investigation by the HHS. The list tracks breaches affecting 500 or more individuals that have occurred since late September 2009, when the HITECH Act-mandated breach notification rule went into effect. More than half of all the major breaches reported since the rule went into effect have involved lost or stolen unencrypted electronic devices or media. By comparison, only about 7 percent have involved a hacker attack. About 22 percent of the breaches have involved a business associate. Source: http://www.govinfosecurity.com/20-million-affected-by-health-breaches-a-4793/op-1

Transportation

NTSB makes ferry safety recommendations. The U.S. National Transportation Safety Board (NTSB) concluded the probable cause of a loss of propulsion control of a Staten Island Ferry in 2010 in New York was the failure of a solenoid. In the wake of its investigation into the accident, the NTSB May 24 made several safety recommendations in a letter to the U.S. Coast Guard Commandant Admiral. "One is the requirement that newly built U.S.-flag passenger vessels with controllable pitch propulsion, including cycloidal propulsion, should be equipped with alarms that audibly and visually alert the operator to deviations between the operator's propulsion and steering commands and the actual propeller response." The NTSB also said that "where technically feasible," these same systems should be retrofitted on existing U.S.-flag passenger vessels. It also recommended the Coast Guard require all U.S.-flag passenger vessel operators to implement safety management systems, taking into account the characteristics, methods of operation, and nature of service of these vessels, and with respect to ferries, the sizes of the ferry systems within which the vessels operate. Source: http://marinelog.com/index.php?option=com_content&view=article&id=2439:ntsb-makes-ferry-safety-recommendations&catid=89:safety-and-security&Itemid=191

Water and Dams

Nothing Significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of

Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168